PCT/JP2004/010401

日　本　国　特　許　庁
JAPAN PATENT OFFICE

26.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００３年１０月　３日

出　願　番　号
Application Number:　特願２００３－３４６２１７

[ST. 10/C]:　［Ｊ Ｐ ２００３－３４６２１７］

出　願　人
Applicant(s):　シャープ株式会社

２００４年　９月　３日

特許庁長官
Commissioner,
Japan Patent Office

小　川　洋

出証番号　出証特２００４－３０７９１８８

【書類名】　特許願
【整理番号】　03J03619
【提出日】　平成15年10月 3日
【あて先】　特許庁長官殿
【国際特許分類】　G11B 11/00
　　G06F 9/06
【発明者】
　【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
　【氏名】　木付　英士
【発明者】
　【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
　【氏名】　大泉　勝志
【発明者】
　【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
　【氏名】　木山　次郎
【特許出願人】
　【識別番号】　000005049
　【氏名又は名称】　シャープ株式会社
　【代表者】　町田　勝彦
【代理人】
　【識別番号】　100079843
　【弁理士】
　【氏名又は名称】　高野　明近
【選任した代理人】
　【識別番号】　100112313
　【弁理士】
　【氏名又は名称】　岩野　進
【手数料の表示】
　【予納台帳番号】　014465
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【包括委任状番号】　0208586

【書類名】特許請求の範囲
【請求項１】
ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置において、前記処理手段は、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴とする記録再生装置。
【請求項２】
請求項１に記載の記録再生装置において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを有し、前記処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールするインストール処理手段を有することを特徴とする記録再生装置。
【請求項３】
請求項２に記載の記録再生装置において、前記インストール処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴とする記録再生装置。
【請求項４】
請求項２又は３に記載の記録再生装置において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記特定領域への書き込み処理を実行できないようにしたことを特徴とする記録再生装置。
【請求項５】
請求項１又は２に記載の記録再生装置において、コンテンツの実行領域であるメモリを有し、前記処理手段は、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードするロード処理手段を有することを特徴とする記録再生装置。
【請求項６】
請求項５に記載の記録再生装置において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴とする記録再生装置。
【請求項７】
請求項１乃至６のいずれか１に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。
【請求項８】
請求項１乃至７のいずれか１に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。
【請求項９】
請求項１乃至８のいずれか１に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。
【請求項１０】
請求項１乃至９のいずれか１に記載の記録再生装置において、前記記録手段は、コンテ

ンツの再生又は実行に必要なプログラム及びデータを１つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段は、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段は、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴とする記録再生装置。

【請求項１１】

請求項１乃至１０のいずれか１に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該再生又は実行中のコンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴とする記録再生装置。

【請求項１２】

請求項１乃至１１のいずれか１に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴とする記録再生装置。

【請求項１３】

請求項１２に記載の記録再生装置において、前記コンテンツの信頼度を、プログラムの記述言語，前記読込手段によって読み込んだコンテンツの読込元となる記録媒体，前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか１又は複数に基づいて設定したことを特徴とする記録再生装置。

【請求項１４】

ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置を用いてコンテンツの構成ファイルへアクセスするためのファイルアクセス方法において、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴とするファイルアクセス方法。

【請求項１５】

請求項１４に記載のファイルアクセス方法において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを前記記録再生装置が備え、前記処理手段が備えるインストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールすることを特徴とするファイルアクセス方法。

【請求項１６】

請求項１５に記載のファイルアクセス方法において、前記インストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴とするファイルアクセス方法。

【請求項１７】

請求項１５又は１６に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記記録手段の特定領域への書き込み処理を実行できないようにしたことを特徴とするファイルアクセス方法。

【請求項１８】

請求項１４又は１５に記載のファイルアクセス方法において、コンテンツの実行領域であるメモリを前記記録再生装置が備え、前記処理手段が備えるロード処理手段が、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードすることを特徴とするファイルアクセス方法。

【請求項１９】
請求項１８に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴とするファイルアクセス方法。
【請求項２０】
請求項１４乃至１９のいずれか１に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。
【請求項２１】
請求項１４乃至２０のいずれか１に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。
【請求項２２】
請求項１４乃至２１のいずれか１に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。
【請求項２３】
請求項１４乃至２２のいずれか１に記載のファイルアクセス方法において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを１つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段が、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段が、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴とするファイルアクセス方法。
【請求項２４】
請求項１４乃至２３のいずれか１に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴とするファイルアクセス方法。
【請求項２５】
請求項１４乃至２４のいずれか１に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴とするファイルアクセス方法。
【請求項２６】
請求項２５に記載のファイルアクセス方法において、前記コンテンツの信頼度を、プログラムの記述言語，前記読込手段によって読み込んだコンテンツの読込元となる記録媒体，前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか１又は複数に基づいて設定したことを特徴とするファイルアクセス方法。

【書類名】明細書
【発明の名称】記録再生装置及びファイルアクセス方法
【技術分野】
【０００１】
本発明は、記録再生装置及びファイルアクセス方法、より詳細には、ＡＶデータやアプリケーションプログラムもしくはアプリケーションプログラムが使用するデータを含むコンテンツを記録，再生，実行可能な記録再生装置及びそのファイルアクセス方法に関する。
【背景技術】
【０００２】
ＤＶＤプレーヤやＤＶＤレコーダ等の普及により、ＨＤＤを内蔵した複合型ＤＶＤレコーダなどが市場に現れはじめた。また、例えばＪａｖａ（Ｒ）言語などの普及により携帯電話などの端末機にもアプリケーションの実行環境が普及し始めた。しかしながら、任意のアプリケーションが実行可能である場合、あらゆる情報へのアクセスを認めることは危険である。そのため、特定のアプリケーション（例えば、ｉアプリ（Ｒ）など）では、信頼できるアプリケーションに限り、携帯電話の保持する電話帳などの各種情報へのアクセスを許可している。
【０００３】
通常、端末にダウンロードされたアプリケーションは、不正な動作を行う可能性があるため、アプリケーションの動作は厳格に制限され、アプリケーションはローカルリソースを用いることができないようになっている。
これに対し、認証モジュールの耐タンパ領域に保持されるアプリケーションの認証情報を用いて、端末にダウンロードされたアプリケーションの認証を行い出所の確認や改ざんが行われていないかどうか確認し、認証されたアプリケーションのみ端末のローカルリソースの利用を許可するようにしたものが開示されている（例えば、特許文献１参照）。
【特許文献１】特開２００３－２２３２３５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ここで、アプリケーションを実行可能な端末装置にローカルストレージを導入し、そのローカルストレージにおいて任意のアプリケーションを実行した場合、そのアプリケーションがコンテンツの作成者の意図に反してコピーや改ざんなどを行う可能性があるため、これに対する対策が必要となる。
また、アプリケーションの入手経路が複数ある場合、信頼性が低く悪意を持ったアプリケーションが実行される可能性がある。そこで、そのアプリケーションの信頼性に応じて各種情報に対するアクセス制限を行う必要がある。
【０００５】
本発明は、上述のごとき実情に鑑みてなされたものであり、ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを記録した外部記録媒体やサーバ装置にアクセスして該コンテンツをローカルストレージに記録すると共に、記録したコンテンツを再生又は実行する記録再生装置において、外部記録媒体又はローカルストレージに記録された任意のコンテンツに対してアクセス制限を付加することにより、そのコンテンツによる不正コピーや改ざんを防止できるようにすること、を目的としてなされたものである。
より具体的には、第１に、インストール対象とするコンテンツのインストール処理やロード処理を自動化し、これらの処理を実行する際に実行中のコンテンツは共通した機能（インストール又はロード）を呼び出すことにより、許可されたインストール対象のコンテンツのみをインストール／ロードして不正なコピーを防止すると共に、実行中のコンテンツに対してアクセス制限することにより改ざんを防止できるようにすること、
第２に、コンテンツの信頼度を判定し、その信頼度に応じて、インストール処理やロード処理とは異なるコンテンツ実行時のデータ読み込み処理、書き出し処理に対してアクセ

ス制限を行うことにより、不正なコピー及び改ざんを防止できるようにすること、をその目的とする。

【課題を解決するための手段】

【０００６】

第１の技術手段は、ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置において、前記処理手段は、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴としたものである。

【０００７】

第２の技術手段は、第１の技術手段において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを有し、前記処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールするインストール処理手段を有することを特徴としたものである。

【０００８】

第３の技術手段は、第２の技術手段において、前記インストール処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴としたものである。

【０００９】

第４の技術手段は、第２又は第３の技術手段において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記特定領域への書き込み処理を実行できないようにしたことを特徴としたものである。

【００１０】

第５の技術手段は、第１又は第２の技術手段において、コンテンツの実行領域であるメモリを有し、前記処理手段は、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードするロード処理手段を有することを特徴としたものである。

【００１１】

第６の技術手段は、第５の技術手段において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴としたものである。

【００１２】

第７の技術手段は、第１乃至第６のいずれか１の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００１３】

第８の技術手段は、第１乃至第７のいずれか１の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００１４】

第９の技術手段は、第１乃至第８のいずれか１の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００１５】
第１０の技術手段は、第１乃至第９のいずれか１の技術手段において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを１つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段は、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段は、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴としたものである。
【００１６】
第１１の技術手段は、第１乃至第１０のいずれか１の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該再生又は実行中のコンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴としたものである。
【００１７】
第１２の技術手段は、第１乃至第１１のいずれか１の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴としたものである。
【００１８】
第１３の技術手段は、第１２の技術手段において、前記コンテンツの信頼度を、プログラムの記述言語，前記読込手段によって読み込んだコンテンツの読込元となる記録媒体，前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか１又は複数に基づいて設定したことを特徴としたものである。
【００１９】
第１４の技術手段は、ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置を用いてコンテンツの構成ファイルへアクセスするためのファイルアクセス方法において、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴としたものである。
【００２０】
第１５の技術手段は、第１４の技術手段において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを前記記録再生装置が備え、前記処理手段が備えるインストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールすることを特徴としたものである。
【００２１】
第１６の技術手段は、第１５の技術手段において、前記インストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴としたものである。
【００２２】
第１７の技術手段は、第１５又は第１６の技術手段において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記記録手段の特定領域への書き込み処理を実行できないようにしたことを特徴としたものである。
【００２３】
第１８の技術手段は、第１４又は第１５の技術手段において、コンテンツの実行領域であるメモリを前記記録再生装置が備え、前記処理手段が備えるロード処理手段が、前記記

録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードすることを特徴としたものである。

【００２４】

第１９の技術手段は、第１８の技術手段において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴としたものである。

【００２５】

第２０の技術手段は、第１４乃至第１９のいずれか１の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００２６】

第２１の技術手段は、第１４乃至第２０のいずれか１の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００２７】

第２２の技術手段は、第１４乃至第２１のいずれか１の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【００２８】

第２３の技術手段は、第１４乃至第２２のいずれか１の技術手段において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを１つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段が、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段が、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴としたものである。

【００２９】

第２４の技術手段は、第１４乃至第２３のいずれか１の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴としたものである。

【００３０】

第２５の技術手段は、第１４乃至第２４のいずれか１の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴としたものである。

【００３１】

第２６の技術手段は、第２５の技術手段において、前記コンテンツの信頼度を、プログラムの記述言語，前記読込手段によって読み込んだコンテンツの読込元となる記録媒体，前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか１又は複数に基づいて設定したことを特徴としたものである。

【発明の効果】

【００３２】

本発明によると、ＡＶデータ又はアプリケーションプログラム／データを含むコンテンツを記録した外部記録媒体やサーバ装置にアクセスして該コンテンツをローカルストレージに記録すると共に、記録したコンテンツを再生又は実行する記録再生装置において、外

部記録媒体又はローカルストレージに記録された任意のコンテンツに対してアクセス制限を付加することにより、そのコンテンツによる不正コピー及び改ざんを防止することができる。

これは、第１に、インストール対象とするコンテンツのインストール処理やロード処理を自動化し、これらの処理を実行する際に実行中のコンテンツは各コンテンツに共通した機能（インストール又はロード）を呼び出すことにより、許可されたインストール対象のコンテンツのみをインストール／ロードすることができるため、不正コピーを防止することができる。また、実行中のコンテンツに対してアクセス制限することによって改ざんを防止することができる。

第２に、コンテンツの信頼度を判定し、その信頼度に応じて、インストール処理やロード処理とは異なるコンテンツ実行時のデータ読み込み処理、書き出し処理に対してアクセス制限することにより、不正コピーや改ざんを防止することができる。これは、すなわち、書き出し処理を制限することによって改ざんを防止し、読み込み及び書き出し処理の組み合わせを制限することによって不正なコピーを防止することができる。

【発明を実施するための最良の形態】

【００３３】

図１は、本発明の一実施形態に係わる記録再生装置の内部構成例について説明するためのブロック図で、図中、１０は記録再生装置で、該記録再生装置１０は、処理部１１，外部デバイスインタフェース１２，デバイスインタフェース１３，ネットワークインタフェース１４，ユーザインタフェース１５から構成される。処理部１１は、各インタフェースから得た情報を利用して、ＡＶデータをデコード、もしくはアプリケーションプログラムを実行する。外部デバイスインタフェース１２は、外部記録媒体１６からＡＶデータやアプリケーションプログラムなどのデータを読み込み、処理部１１に引き渡すことが出来る。ここで、外部記録媒体１６とは、例えば、ＣＤ－ＲＯＭ，ＣＤ－Ｒ（ＲＷ），ＤＶＤ－ＲＯＭなどを含む光ディスクや、メモリカードなどを指す。この外部記録媒体１６に記録されているデータは、記録再生装置１０以外で記録されたものであってもよい。

【００３４】

以下の説明において、意味のあるまとまりを持ったＡＶデータもしくはアプリケーションプログラム／データをコンテンツとして定義する。また、ＡＶデータとは映像、音声、もしくはその両方を再生するために必要な情報の全てもしくは一部を指す。また、アプリケーションプログラムとはアプリケーションの実行に必要な情報の全てもしくは一部を指す。上記コンテンツは、例えば、１タイトルに相当するＡＶデータを構成するファイル全体や、１つのゲーム又はアプリケーションを構成するプログラムファイル及びデータファイル全体から構成されている。

【００３５】

ネットワークインタフェース１４は、ネットワーク１７を介して、ネットワーク１７に接続されているサーバ装置（図示せず）からデータをダウンロードし、処理部１１に引き渡すことが出来る。本例では、外部記録媒体１６とネットワーク１７のいずれからもデータを取得することが出来る構成としているが、これに限定されず何れか一方だけであっても良い。

【００３６】

ユーザインタフェース１５は、ディスプレイ１８、コントローラ１９に接続されている。処理部１１は、ユーザインタフェース１５を通じてＡＶデータなどをディスプレイ１８に出力してユーザにＡＶデータを視聴させることが出来る。また、コントローラ１９から入力されるユーザの要求は、ユーザインタフェース１５を介して処理部１１に伝えられる。

デバイスインタフェース１３は、記録媒体（ローカルストレージ）２０からデータを読み込んだり、記録媒体２０にデータを書き出したりすることが出来る。ここで、記録媒体２０は、内蔵又は外付けのハードディスク装置や、記録可能な光ディスクやメモリカードなどの記録媒体であってもよい。記録媒体２０（以下、記録装置２０で代表する）に記録

されているデータは、記録再生装置１０で記録されたデータである。

【００３７】

処理部１１は、予め用意されたコンテンツ（ＡＶデータ又はアプリケーションプログラム）もしくはいずれかのインタフェースを経由して読み込んだコンテンツを実行し、その処理のひとつとしてファイルアクセス処理を行う。

【００３８】

まず、記録再生装置１０のファイルアクセス処理には次の３種類がある。

（処理１）コンテンツの全体又は一部を外部記録媒体１６もしくはネットワーク１７経由でサーバ装置から読み込み、記録装置２０に識別可能な形式で記録するインストール処理

（処理２）コンテンツを再生又は実行するために必要なプログラムやデータを記録装置２０又は外部記録媒体１６又はネットワーク１７経由でサーバ装置から内部メモリ上に読み込むロード処理

（処理３）コンテンツが自身で生成したデータを書き出す処理及び読み込む処理

【００３９】

本発明は、上記ファイルアクセス処理に対して不正なコピー及び改ざんを防止するために以下のようにアクセス制限を付加するものである。

【００４０】

まず、上記（処理１）のコンテンツを外部記録媒体１６もしくはネットワーク１７経由でサーバ装置から読み込み、記録装置２０に識別可能な形式で記録するインストール処理について説明する。

ここで、外部記録媒体１６もしくはネットワーク１７経由でアクセス可能なサーバ装置にあるデータのうち、そのデータ提供者が認めたもののみをインストールし、それ以外のデータのインストール、つまり不正なコピーを防止する必要がある。また、インストールしたデータに対して改ざんが行われないようにする必要がある。そこで、インストールに必要な処理を共通化して定義し、実行中のコンテンツは、その共通化した処理にのみトリガを与える。このとき、簡単にインストールを実現するために、意味を持ったひとまとまりのコンテンツ（ＡＶデータ又はアプリケーションプログラム）を管理する管理情報がインストール元にあることが望ましい。

【００４１】

図２は、コンテンツの全体又は一部に対して共通化されたインストール処理の一例を説明するためのフロー図である。まず、記録再生装置１０は、インストール処理の開始に際し（ステップＳ１）、外部記録媒体１６もしくはネットワーク１７経由でアクセス可能なサーバ装置に対してインストールしたいコンテンツの全体又は一部を指定する（ステップＳ２）。そのコンテンツの全体又は一部が、コンテンツ提供者がインストールを許可しているコンテンツであるかどうかを確認する（ステップＳ３）。ここで、具体的な確認方法として、例えば、上記コンテンツの全体又は一部のフォーマットやメタデータなどから判断するようにしてもよい。

【００４２】

上記ステップＳ３において、インストールを許可されたコンテンツの全体又は一部でない場合（ＮＯの場合）エラーを返して終了する（ステップＳ４）。また、上記ステップＳ３において、インストールを許可されたコンテンツの全体又は一部であった場合（ＹＥＳの場合）、記録装置２０を確認する。これは、記録装置２０に十分な空き容量があり、また、すでに記録されているコンテンツの全体又は一部と不整合を起こす可能性が無いかどうかを確認する（ステップＳ５）。

上記ステップＳ５において、記録装置２０の容量が足らない、もしくは、すでに記録されているコンテンツの全体又は一部と不整合を起こす可能性がある場合（ＮＯの場合）、エラーを返して終了する（ステップＳ６）。また、上記ステップＳ５において、記録装置２０に記録可能である場合（ＹＥＳの場合）、インストールするコンテンツの全体又は一部を特定の管理情報と共に記録装置２０に記録し（ステップＳ７）、処理成功を返して終了する（ステップＳ８）。ここで、特定の管理情報とは、記録装置２０上で、インストー

ル済みのコンテンツの全体又は一部を区別して管理するための情報で、コンテンツの全体又は一部の整合性のための情報にもなり、コンテンツの全体又は一部の削除（アンインストール）を行う際にも利用する情報である。

【００４３】

図３は、コンテンツの全体又は一部に対して共通化された削除（アンインストール）処理の一例を説明するためのフロー図である。まず、記録再生装置１０は、アンインストール処理の開始に際し（ステップＳ１１）、記録装置２０上のアンインストールしたいコンテンツの全体又は一部を指定する（ステップＳ１２）。次に、そのコンテンツの全体又は一部が記録装置２０にあるかどうかを確かめる（ステップＳ１３）。

上記ステップＳ１３において、コンテンツの全体又は一部が記録装置２０に無い場合（ＮＯの場合）、エラーを返して終了する（ステップＳ１４）。また、上記ステップＳ１３において、コンテンツの全体又は一部が記録装置２０にある場合（ＹＥＳの場合）、そのコンテンツの全体又は一部と共に記録した特定の管理情報を用いてコンテンツの全体又は一部に含まれる全てのファイルとその管理情報を記録装置２０から削除し（ステップＳ１５）、処理成功を返して終了する（ステップＳ１６）。

【００４４】

次に、上記（処理２）のコンテンツを再生又は実行するために必要なプログラムやデータを記録装置２０又は外部記録媒体１６又はネットワーク１７経由でサーバ装置から内部メモリ上に読み込むロード処理について説明する。ここで、ロード処理においても、インストール処理と同様に、ロードに必要な処理を共通化して定義し、実行中のコンテンツは、その共通化した処理にのみトリガを与える。

ロード処理において、記録装置２０、外部記録媒体１６、もしくはネットワーク１７経由でアクセス可能なサーバ装置のいずれからも同様に、コンテンツを再生又は実行するために内部メモリ上にプログラムやデータをロードする。このロード処理は、読み込み処理のみで、書き出し処理を必要としないので、直接、改ざんや不正コピーが行われることはない。

【００４５】

次に、（処理３）のコンテンツ自身で生成したデータを書き出す処理及び読み込む処理について説明する。

コンテンツに提供されるファイルシステムは、基本的に記録装置２０、外部記録媒体１６、もしくはネットワーク１７経由でアクセス可能なサーバ装置のいずれにも同様にアクセスすることができる。ただし、読み込み専用の記録媒体に書き出すことは出来ない。例えば、外部記録媒体１６がＣＤ－ＲＯＭのような読み込み専用の記録媒体であった場合、上記ファイルシステムを用いて外部記録媒体１６に書き出すことは出来ない。ここで、上記ファイルシステムには、次の条件が付加される。

・上記（処理２）によって処理部１１の内部メモリにロードされたコンテンツ（ＡＶデータ及びアプリケーションプログラム）にはアクセスできない。

これによって、コンテンツが、ロードされたデータを読み込んだり、変更を加えることを禁止することができる。

【００４６】

また、上記コンテンツのファイルシステムが、外部記録媒体１６に記録された他の又は全てのコンテンツにアクセスできないようにしてもよく、また、記録装置２０にインストールされた他の又は全てのコンテンツにアクセスできないようにしてもよい。また、上記ファイルシステムの記録装置２０又は外部記録媒体１６又はネットワーク１７経由したサーバ装置へのアクセス全てを禁止するようにしてもよい。

【００４７】

ただし、上記コンテンツは、（処理１）を呼び出すインストール命令及びアンインストール命令、もしくは（処理２）のロード処理を含む再生命令及びアプリケーション実行命令を発行することは可能である。

【００４８】

これまでの処理を図４にまとめる。

図４は、図１に示した処理部１１の詳細構成例を説明するためのブロック図で、処理部１１は、アプリケーション実行部１１ａ，インストール処理部１１ｂ，ロード処理部１１ｃ及びメモリ１１ｄを含むものとする。記録媒体２０$_1$、２０$_2$は、図１に示した記録装置２０に含まれる異なる記録部分としてもよく、また、独立した記録媒体であってもよい。また、処理部１１は、外部記録媒体１６もしくはネットワーク１７に接続されたサーバ装置（以下、外部記録媒体１６で代表する）にアクセス可能とする。尚、本実施形態では、図１に示した各インタフェースは省略されている。

【００４９】

図４において、アプリケーション実行部１１ａで実行されるアプリケーションは、基本的に記録媒体２０$_1$、２０$_2$、外部記録媒体１６に記録されているコンテンツ（ＡＶデータもしくはアプリケーションプログラム）にアクセス可能とし、外部記録媒体１６への記録も可能である。また、上記アプリケーションはインストール処理部１１ｂ及びロード処理部１１ｃに命令を発行することが出来る。

【００５０】

インストール処理部１１ｂは、外部記録媒体１６に記録されているコンテンツを読み込み、記録媒体２０$_2$に書き出すことが出来る。また、記録媒体２０$_2$に記録されているコンテンツを削除することが出来る。このインストール処理部１１ｂは、コンテンツからのインストール命令を受け付けて、インストール処理を実行する。従って、インストール処理時に、コンテンツは外部記録媒体１６、記録媒体２０$_2$に直接アクセスすることはできない。

【００５１】

ロード処理部１１ｃは、外部記録媒体１６もしくは記録媒体２０$_2$からコンテンツを読み込み、メモリ１１ｄに書き出すことが出来る。このロード処理部１１ｃは、コンテンツからのロード命令を受け付けて、ロード処理を実行する。従って、ロード処理時に、コンテンツは外部記録媒体１６、記録媒体２０$_2$に直接アクセスすることはできない。

【００５２】

メモリ１１ｄは、ロード処理部１１ｃによって書き出されたコンテンツのみを記憶する。これらはアプリケーション実行部１１ａで実行されるアプリケーション自身であり、アプリケーションが使用する変数などはこの領域には記憶しない。また、このアプリケーションがメモリ１１ｄに記憶されたデータを参照することは出来ない。

【００５３】

アプリケーション実行部１１ａで実行されるアプリケーションプログラム（又はＡＶデータ、以下、アプリケーションプログラムで代表する）によっては外部記録媒体１６に記録されているデータを、記録媒体２０$_1$，２０$_2$や、他の外部記録媒体などにコピーすることが出来る。ここで、外部記録媒体１６に記録されているデータの作者もしくは提供者が、そのデータのコピーを望んでおらず、その正当性を認めていない場合がある。このように不正なコピーを行うアプリケーションプログラムが存在する可能性を考慮し、アプリケーションプログラムの信頼性を評価し、それに応じて、アクセスを制限する方法について説明する。

【００５４】

図５は、アプリケーションプログラムの信頼性に応じたアクセス制限の一例を示した図である。例えば、最も信頼できるアプリケーションプログラムであれば、アプリケーション実行部１１ａに許可された全てのアクセスを可能とする。やや信頼できるアプリケーションプログラムであれば、外部記録媒体１６及び記録媒体２０$_2$への書き出しのみを禁止する。次に信頼できるアプリケーションプログラムであれば、外部記録媒体１６及び記録媒体２０$_2$からの読み込みのみを許可する。あまり信頼できないアプリケーションプログラムであれば、外部記録媒体１６及び記録媒体２０$_2$へのアクセスを禁止する。ほとんど信頼できないアプリケーションであれば、全てのアクセスを禁止する。ただし、アプリケーションプログラムの信頼性とアクセス制限の組み合わせは上記例に限定されるものでは

ない。また、外部記録媒体１６及び記録媒体２０$_2$を同一に扱うように制限されるものではない。

【００５５】

また、アプリケーションプログラムの信頼性の評価方法について以下に例を示す。

例えば、アプリケーションプログラムのメタデータを照合するなどの認証処理によって判断する方法がある。また、複数のアプリケーションプラットフォームを持っている場合、アプリケーションプログラムがいずれのプラットフォーム上で動作するかによってその信頼性を判断する方法がある。例えば、ＡＶデータに含まれるマクロ言語の実行環境は、あまり高度なプログラムを組むことは出来ない。そのため、不正な処理を実現することが出来ないという理由で、信頼性が高いと判断することも出来る。

【００５６】

さらに、外部記録媒体１６が特定のメーカにしか製造できない読み込み専用の記録媒体であったとする。その場合、外部記録媒体１６からロードされるアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。同様に、記録装置２０にインストールされたアプリケーションプログラムのインストール元が、特定のメーカにしか製造できない読み込み専用の記録媒体であった場合、そのアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。さらに、ネットワーク上のサーバ装置のうち、特定のメーカにしか製造できない読み込み専用の記録媒体にそのアドレスが信頼に足ると記録されていれば、そのアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。このような条件を組み合わせることによって、アプリケーションプログラムの信頼性を評価することが出来る。

【００５７】

次に、これまで説明した記録再生装置１０について具体的な例を挙げて説明する。

対象となる記録再生装置１０は、ＤＶＤプレーヤのようにＲＯＭディスクに記録されたＡＶデータを再生する機能を有している。また、ＡＶデータの他にＪａｖａ（Ｒ）言語で書かれたアプリケーションプログラムをＲＯＭディスクから読み込んでアプリケーションを実行することが出来る。ＲＯＭディスクに加えてネットワークインタフェースを通じて、ＡＶデータやアプリケーションプログラムを実行することも出来る。さらに、記録可能媒体へのインタフェースを持ち、上記ＡＶデータやアプリケーションプログラムをインストールし、上記記録可能媒体から読み込んで再生・実行することが出来る。また、アプリケーションプログラムが任意のデータを上記記録可能媒体に書き出し、読み込むことが出来る。

【００５８】

ここで、本実施形態では、ＡＶデータとアプリケーションプログラムの双方を再生・実行可能な記録再生装置１０を例に挙げているが、アプリケーションプログラムのみ実行可能な機器であっても良い。また、本例のアプリケーションプログラムの記述言語はＪａｖａ（Ｒ）言語に限定されず、例えばＢＡＳＩＣ言語、Ｃ言語、また用意されたマクロ言語などプログラムデータを読み込んで実行可能な環境であればいずれの言語でも良い。また、本例では、ＡＶデータやアプリケーションプログラムを読み込むインタフェースとしてＲＯＭディスクとネットワーク双方のインタフェースを用意したが、何れか一方だけであっても良い。

【００５９】

ＤＶＤなどのＲＯＭディスクに記録されたコンテンツは、オーサもしくはプロバイダの意図によって、複製や改造が認められていないものが多い。これらを含む同様の許可されていない複製や改造に対して、本発明の記録再生装置１０を用いて、コンテンツの複製や改造を防止するための方法について説明する。

【００６０】

まず、装置構成について前述した図１に基づいて説明する。記録再生装置１０において、外部記録媒体１６はＲＯＭディスク１６、記録装置２０はハードディスク２０、外部デバイスインタフェース１２はＲＯＭディスクインタフェース１２、デバイスインタフェー

ス１３はハードディスクインタフェース１３として読み替えるものとする。

【００６１】

処理部１１は各インタフェースから得た情報を利用して、ＡＶデータをデコード、もしくはアプリケーションプログラムを実行する。ＲＯＭディスクインタフェース１２は、ＲＯＭディスク１６からＡＶデータやアプリケーションプログラムなどのデータを読み込み、処理部１１に引き渡すことが出来る。ネットワークインタフェース１４は、ネットワーク１７を介してサーバ装置（図示せず）からデータをダウンロードし、処理部１１に引き渡すことが出来る。

【００６２】

ユーザインタフェース１５は、ディスプレイ１８、コントローラ１９に接続されている。処理部１１は、ユーザインタフェース１５からＡＶデータをディスプレイ１８に出力し、ユーザにＡＶデータを視聴させることが出来る。また、コントローラ１９から入力されたユーザの要求は、ユーザインタフェース１５を介して処理部１１に伝えられる。ハードディスクインタフェース１３は、ハードディスク２０からデータを読み込んだり、ハードディスク２０にデータを書き出したりすることが出来る。ただし、本例のハードディスク２０に限定されず、ＲＡＭディスクやメモリカードなどでも良い。また、ハードディスク２０は記録再生装置１０に内蔵あるいは外付けのいずれの形態としても良い。

【００６３】

処理部１１は、予め用意されたコンテンツ（ＡＶデータ又はアプリケーションプログラム）、もしくは、いずれかのインタフェースを経由して読み込んだコンテンツを実行し、その処理のひとつとしてファイルアクセス処理を行う。

【００６４】

まず、ＲＯＭディスクインタフェース１２もしくはネットワークインタフェース１４を介して読み込んだコンテンツ（ＡＶデータ又はアプリケーションプログラム）を、ハードディスクインタフェース１３を介してハードディスク２０にインストールする処理について説明する。

【００６５】

ここでインストールとは、ＲＯＭディスク１６もしくはネットワーク１７を介してアクセス可能なサーバ装置において、ハードディスク２０にコピーが認められたコンテンツを、識別可能な形式でハードディスク２０に記録することをいう。ここで、インストール可能なひとまとまりのコンテンツをパッケージと呼ぶことにする。例えば、ひとつの映画であり、トレーラー（映画の予告編）であり、また、ゲームである。また、パッケージは、ＲＯＭディスク１６のコンテンツを補強するものであっても良い。例えば、ＲＯＭディスク１６のコンテンツには含まれない言語の字幕情報と、それを再生可能にする管理情報などである。

【００６６】

ここで、ＲＯＭディスク１６においてインストールが認められているコンテンツを判別する方法の一例を下記の図６に基づいて説明する。

図６は、ＲＯＭディスク１６に記録されているファイル構成の一例を示した図である。

図６（Ａ）に示すＲＯＭディスク１６のファイル構成において、ルートディレクトリ３１の下には、ｖｉｄｅｏという名前のフォルダ３２と、ｉｎｓｔａｌｌ．ｉｎｆｏという名前のファイル３５と、ｐａｃｋａｇｅという名前のフォルダ３６とがある。ここでｖｉｄｅｏフォルダ３２は、このＲＯＭディスク１６のＡＶデータを再生するときに自動的に参照されるフォルダである。このフォルダ３２内のｉｎｄｅｘ０１．ｉｎｆｏという名前のファイル３３は再生順序をコントロールする管理情報ファイルであり、ｃｏｎｔｅｎｔ０１．ｍｐｇという名前のファイル３４はＡＶデータの実体が記録されたファイルである。例えば、ｉｎｄｅｘ０１．ｉｎｆｏファイル３３がロードされ、その記述に従ってｃｏｎｔｅｎｔ０１．ｍｐｇファイル３４が再生される。ここで、ｉｎｄｅｘ０１．ｉｎｆｏファイル３３は、再生可能なＡＶデータを管理しているが、実行可能なプログラムファイルを管理するものであっても良い。もしくは、ファイル３３自体が実行可能なプログラム

ファイルであっても良い。また、ひとつの管理情報ファイルが複数のＡＶデータやプログラムファイルを管理していても良い。さらに、管理情報ファイルが複数あっても良い。その場合、デフォルトでロードされるファイル名が特定される必要がある。ｉｎｓｔａｌｌ．ｉｎｆｏファイル３５は、インストールが認められているファイルを管理している。

【００６７】

図６（Ｂ）は、ｉｎｓｔａｌｌ．ｉｎｆｏファイル３５の内容の一例を示す図である。コピーが認められているファイルへのパスと、管理用かつ表示用のタイトルと、表示用のイメージファイルへのパスが記録されている。ｐａｃｋａｇｅフォルダ３６には、ｉｎｄｅｘ０１．ｉｎｆｏという名前のファイル３７と、ｃｏｎｔｅｎｔ０１．ｍｐｇという名前のファイル３８と、ｉｍａｇｅ．ｊｐｇという名前のファイル３９とが含まれている。ｉｎｄｅｘ０１．ｉｎｆｏファイル３７は、再生順序をコントロールする管理情報ファイルであり、ｃｏｎｔｅｎｔ０１．ｍｐｇファイル３８はＡＶデータの実体が記録されたファイルである。

【００６８】

図６（Ｂ）に示すコピーが認められているファイルは、ｉｎｄｅｘ０１．ｉｎｆｏファイル３７とｃｏｎｔｅｎｔ０１．ｍｐｇファイル３８であり、表示用のイメージファイルは、ｉｍａｇｅ．ｊｐｇファイル３９であることがわかる。表示用のイメージファイルとは、インストールされたパッケージをユーザに提示する際の代表画像であり、ＤＶＤディスクなどのケース表面に印刷されているような画像が考えられる。そして、ｉｎｓｔａｌｌ．ｉｎｆｏファイル３５に登録されているファイルがインストールの対象となり、登録されていないファイルは、インストールの対象とはならない。また、上記例では、ｉｎｓｔａｌｌ．ｉｎｆｏファイル３５が管理するのはひとつのパッケージであるが、これに限定されず複数のパッケージを管理しても良い。もしくは、複数のインストール情報ファイルを作成するようにしても良い。

【００６９】

図７は、ハードディスク２０に記録されているファイル構成の一例を示した図である。ルートディレクトリ４１の下にｐａｃｋａｇｅ．ｌｉｓｔという名前のファイル４２がある。ｐａｃｋａｇｅ．ｌｉｓｔファイル４２は、インストールされた各パッケージを管理する管理情報ファイルであり、また、各パッケージのフォルダをＲＯＭディスク１６のｖｉｄｅｏフォルダと等価に扱うための変換テーブルである。インストールされたパッケージは、システムが用意したフォルダにｖｉｄｅｏフォルダと同様の形式で記録される。例えば、ｐｋｇ００１フォルダ４３にｉｎｄｅｘ０１．ｉｎｆｏファイル４４と、ｃｏｎｔｅｎｔ０１．ｍｐｇファイル４５のように記録される。これらのデータの再生手段については前述したＲＯＭディスクコンテンツの再生手順と同様である。また、表示用のイメージファイルも同じフォルダに記録される。例えば、ｉｍａｇｅ．ｊｐｇファイル４６である。そしてこれらのデータへのパスが、管理用のタイトルと関連付けられて、ｐａｃｋａｇｅ．ｌｉｓｔファイル４２に記録されている。

【００７０】

また、同様に、ｐｋｇ００２フォルダ４７にはｉｎｄｅｘ０１．ｉｎｆｏファイル４８と、ｃｏｎｔｅｎｔ０１．ｍｐｇファイル４９のように記録される。表示用のイメージファイルも同じフォルダに記録される。例えば、ｉｍａｇｅ．ｊｐｇファイル５０である。

【００７１】

上記の処理はアプリケーションプログラムからインストールコマンドがコールされることによって実行される。インストールコマンドは、例えばデバイスを指定することで、自動的に処理される。デバイスに複数のパッケージが存在するのであれば、管理用のタイトルを取得するコマンドと、管理用のタイトルを指定するインストールコマンドを併用することで実現できる。

【００７２】

また、必要であればパッケージのバージョンアップを導入しても良い。同一の管理用タイトルで管理されるパッケージに異なるバージョンが存在する場合に、古いバージョンの

パッケージを新しいバージョンのパッケージに入れ替える処理を自動的に行う。そしてアプリケーションプログラムは、バージョンアップコマンドをコールすることによって実現する。必要に応じて、図６（Ａ）に示したｉｎｓｔａｌｌ．ｉｎｆｏファイル３５や、図７に示したｐａｃｋａｇｅ．ｌｉｓｔファイル４２にパッケージ及び各ファイルのバージョンを記録する。

【００７３】

次に、ＲＯＭディスク１６、もしくはネットワーク１７を介してアクセス可能なサーバ装置、もしくはハードディスク２０のコンテンツをロードして、再生・実行する方法について以下に説明する。

コンテンツの再生は、管理情報ファイルを指定することで行われる。この管理情報ファイルの指定方法は２つあり、デバイス上の管理情報ファイルを直接指定する方法と、デバイスにデフォルトで指定されている管理情報ファイルの指定としてデバイスを指定する方法である。ここで、再生・実行ファイルの指定方法について下記の図８に基づいて説明する。

【００７４】

図８は、ＲＯＭディスク１６及びハードディスク２０に記録されているファイル構成の他の例を示した図である。

図８（Ａ）に示すＲＯＭディスク１６のファイル構成において、ルートディレクトリ６１以下にはｖｉｄｅｏフォルダ６２があり、ｉｎｄｅｘ０１．ｉｎｆｏファイル６３は、ｃｏｎｔｅｎｔ０１．ｍｐｇファイル６４とｃｏｎｔｅｎｔ０２．ｍｐｇファイル６５を、ｉｎｄｅｘ０２．ｉｎｆｏファイル６６は、ｃｏｎｔｅｎｔ０３．ｍｐｇファイル６７を、ｏｔｈｅｒｓ６８以下のｉｎｄｅｘ０４．ｉｎｆｏファイル６９は、ｃｏｎｔｅｎｔ０４．ｍｐｇファイル７０をそれぞれ管理している。

【００７５】

管理情報ファイルを直接指定する場合、デバイスとしてＲＯＭディスク１６を指定して、フルパスで管理情報ファイル、例えばｉｎｄｅｘ０２．ｉｎｆｏファイル６６を指定する。また、ｖｉｄｅｏフォルダ６２以下のファイルでなくても、例えばｉｎｄｅｘ０４．ｉｎｆｏファイル６９を指定することが出来る。本例の場合、デフォルトで指定されているファイルは、ｖｉｄｅｏフォルダ６２以下のｉｎｄｅｘ０１．ｉｎｆｏファイル６３であるので、ＲＯＭディスクインタフェース１２を指定するとｉｎｄｅｘ０１．ｉｎｆｏファイル６３が再生・実行対象のファイルとして指定されたことになる。

【００７６】

また、ネットワーク１７を介したサーバ装置に対しても上記と同様の処理が可能である。例えば、サーバ装置の管理情報ファイルを直接指定することが出来る。ｈｔｔｐプロトコルであれば、例えば「ｈｔｔｐ：／／ｗｗｗ．ｓｈａｒｐ．ｃｏ．ｊｐ／ｉｎｄｅｘ０５．ｉｎｆｏ」などと指定することができる。

【００７７】

図８（Ｂ）に示すハードディスク２０のファイル構成において、ハードディスクの扱い方の一例として、ハードディスク２０の各パッケージを各管理用タイトルで管理される仮想デバイスとして認識する。ルートディレクトリ７１以下、例えば、ｐｋｇ００１フォルダ７３とそれ以下のファイル（ｉｎｄｅｘ０１．ｉｎｆｏファイル７４，ｃｏｎｔｅｎｔ０１．ｍｐｇ７５，ｃｏｎｔｅｎｔ０２．ｍｐｇ７６，ｉｎｄｅｘ０２．ｉｎｆｏファイル７７，ｃｏｎｔｅｎｔ０３．ｍｐｇ７８，ｉｍａｇｅ．ｊｐｇ７９）は、管理用タイトル「ＡＡＡ」に関連付けられたパッケージ、ｐｋｇ００２フォルダ８０とそれ以下のファイル（ｉｎｄｅｘ０１．ｉｎｆｏファイル８１，ｃｏｎｔｅｎｔ０１．ｍｐｇ８２，ｉｍａｇｅ．ｊｐｇ８３）は、管理用タイトル「ＢＢＢ」に関連付けられたパッケージであるとｐａｃｋａｇｅ．ｌｉｓｔファイル７２に記録されているものとする。

ここで、管理情報ファイルを直接指定する場合、例えばデバイスとして「ＡＡＡ」を指定して、フルパスで管理情報ファイルｉｎｄｅｘ０２．ｉｎｆｏファイル７７を指定する。また、デバイス「ＢＢＢ」のみを指定するとデフォルトに指定されているｉｎｄｅｘ０

１．ｉｎｆｏファイル８１が指定されたことになる。

【００７８】

上記のように指定されたコンテンツは、再生・実行用の特定のメモリに必要なデータをロードすることによって実行される。この処理はアプリケーションプログラムから再生コマンド、もしくは実行コマンドがコールされることによって実行される。

【００７９】

次に、任意のアプリケーションプログラムに許可されたアクセスについて説明する。まず、任意のアプリケーションプログラムは、ロードされたメモリ上のコンテンツ（ＡＶデータ又はアプリケーションプログラム）にアクセスすることは出来ない。また、アプリケーションプログラムは、アプリケーションが生成したデータを読み込み、書き込みするための特定の領域をハードディスク２０に有している。ここで、特定の領域の例を、下記の図９に基づいて説明する。

【００８０】

図９は、ハードディスク２０に記録されているファイル構造の他の例を示した図である。ルートディレクトリ９１以下、ｐａｃｋａｇｅ．ｌｉｓｔ９２，ｐｋｇ００１フォルダ９３，ｉｎｄｅｘ０１．ｉｎｆｏファイル９４，ｃｏｎｔｅｎｔ０１．ｍｐｇファイル９５，ｉｍａｇｅ．ｊｐｇファイル９６，ｐｋｇ００２フォルダ９７，ｉｎｄｅｘ０１．ｉｎｆｏファイル９８，ｃｏｎｔｅｎｔ０１．ｍｐｇファイル９９，ｉｍａｇｅ．ｊｐｇファイル１００まではこれまで説明した通りである。本例では、加えてｓａｖｅｄａｔａフォルダ１０１を有し、ｓａｖｅｄａｔａフォルダ１０１以下のファイルをｓａｖｅｄａｔａ．ｌｉｓｔファイル１０２が管理する。ｓａｖｅｄａｔａ．ｌｉｓｔファイル１０２はｓａｖｅｄａｔａフォルダ１０１以下のファイルを管理する管理ファイルである。ｓａｖｅｄａｔａフォルダ１０１以下には、ｓａｖｅｄａｔａ．ｌｉｓｔ（管理情報）ファイル１０２によって各アプリケーションプログラムに関連付けられた００１．ｄａｔファイル１０３と００２．ｄａｔファイル１０４とを有する。任意のアプリケーションプログラムに関連付けられたファイルが特定の領域に相当する。つまり、各アプリケーションプログラムはｓａｖｅｄａｔａ．ｌｉｓｔ（管理情報）ファイル１０２に管理され、ｓａｖｅｄａｔａフォルダ１０１以下に用意されたファイルにのみ読み込み、書き出しのアクセスができる。また、各パッケージを形成するフォルダに対してはロード処理と同様のアクセス手順で外部記録媒体１６と同じようにアクセスすることができる。

【００８１】

さらに、任意のアプリケーションプログラムは、ＲＯＭディスク１６もしくはネットワーク１７を介してアクセス可能なサーバ装置のデータを読み込むことが出来る。

【００８２】

これまでのアクセス制限で、少なくとも再生・実行のためにメモリ上にロードされたデータを改ざんすることを禁止することが出来る。しかし、任意のアプリケーションプログラムが、ＲＯＭディスク１６もしくはハードディスク２０もしくはネットワーク１７を介してアクセス可能なサーバ装置のデータを読み込み、ハードディスク２０に記録することが出来る。これは、記録されたデータの再生もしくは実行の可否に関わらず、認められていないコピーである可能性がある。

【００８３】

ここで、アプリケーションプログラムの信頼性に応じて、アクセスの制限を変える方法を適用する。まずアプリケーションの信頼性を判定する方法の例を以下に示す。

例えば、第１に、ＲＯＭディスク１６が一般のユーザにとって製造困難である場合、特定のメーカによってのみ製造されることになる。つまり、それらのメーカが信頼に足りることがわかれば、ＲＯＭディスク１６のデータは信頼できる。また、インストールされたデータを改ざんされる恐れが無いことから、ＲＯＭディスク１６からインストールされたデータも信頼できる。第２に、ＲＯＭディスク１６に記録されたネットワークアドレスが指し示すサーバ装置のデータ及びそこからインストールされたデータも信頼できる。ただし、ネットワーク自体を偽称することによって問題のある可能性があるのでやや信頼性が

下がる。そして第３に、不特定のネットワークアドレスが指し示すサーバ装置のデータ及びそこからインストールされたデータは最も信頼できないものと判断する。

【００８４】

インストールされたデータに関して信頼性の判定基準が必要である場合、ｐａｃｋａｇｅ．ｌｉｓｔファイルなどの管理情報に上記の３つの信頼性レベルを表すフラグを記録しても良い。

【００８５】

図１０は、３つの信頼性レベルに対して、３つのアクセス制限レベルを適用する一例を示す図である。まず、ＲＯＭディスク１６への書き出しは、もともと不可能である。最も信頼できる第１の信頼性レベルに相当するアプリケーションプログラムは、不正な処理を行わないと信頼できるとして、ＲＯＭディスク１６からの読み込み、ハードディスク２０のｓａｖｅｄａｔａフォルダ１０１以下のアプリケーションに対応したファイルへの書き出しと読み込み、ハードディスク２０のパッケージ（例えば、ｐｋｇ００１フォルダ９３）からの読み込みのアクセスが認められ、ハードディスク２０のパッケージ（例えば、ｐｋｇ００１フォルダ９３）への書き出しは禁止される。

【００８６】

逆に最も信頼できない第３の信頼性レベルに相当するアプリケーションプログラムは、ＲＯＭディスク１６、ハードディスク２０双方へのアクセスを全て禁止される。

そして、やや信頼できる第２の信頼性レベルのアプリケーションプログラムは、以下のいずれかの制限を受ける。ひとつは、ＲＯＭディスク１６からの読み込み、ハードディスク２０のパッケージ（例えば、ｐｋｇ００１フォルダ９３）への書き出しと読み込みを禁止する。もうひとつは、ハードディスク２０のｓａｖｅｄａｔａフォルダ１０１以下のアプリケーションに対応したファイルへの書き出しと読み込み、ハードディスク２０のパッケージ（例えば、ｐｋｇ００１フォルダ９３）への書き出しを禁止する。この何れかを適用することによって、ＲＯＭディスク１６からハードディスク２０へのデータコピーを不可能とする。

【００８７】

さらに、外部記録媒体（以下、外部記録媒体Ａ）からロードされたアプリケーションがアクセスできる外部記録媒体を、上記外部記録媒体Ａに限定する。また、インストールされたパッケージ（以下、パッケージＢ）からロードされたアプリケーションがアクセスできるパッケージを、上記パッケージＢに限定する。このような機能を実装することで不正コピーの可能性を防止するようにしてもよい。また、アプリケーションからパッケージへの書き込みを禁止することで不正な改ざんを防止するようにしてもよい。

【産業上の利用可能性】

【００８８】

本発明の記録再生装置及びファイルアクセス方法は、各種アプリケーションプログラムを実行可能な携帯端末装置や、ＨＤＤを内蔵したＤＶＤレコーダなどに好適に利用することができる。

【図面の簡単な説明】

【００８９】

【図１】本発明の一実施形態に係わる記録再生装置の内部構成例について説明するためのブロック図である。

【図２】コンテンツの全体又は一部に対して共通化されたインストール処理の一例を説明するためのフロー図である。

【図３】コンテンツの全体又は一部に対して共通化された削除（アンインストール）処理の一例を説明するためのフロー図である。

【図４】図１に示した処理部の詳細構成例を説明するためのブロック図である。

【図５】アプリケーションプログラムの信頼性に応じたアクセス制限の一例を示した図である。

【図６】ＲＯＭディスクに記録されているファイル構成の一例を示した図である。

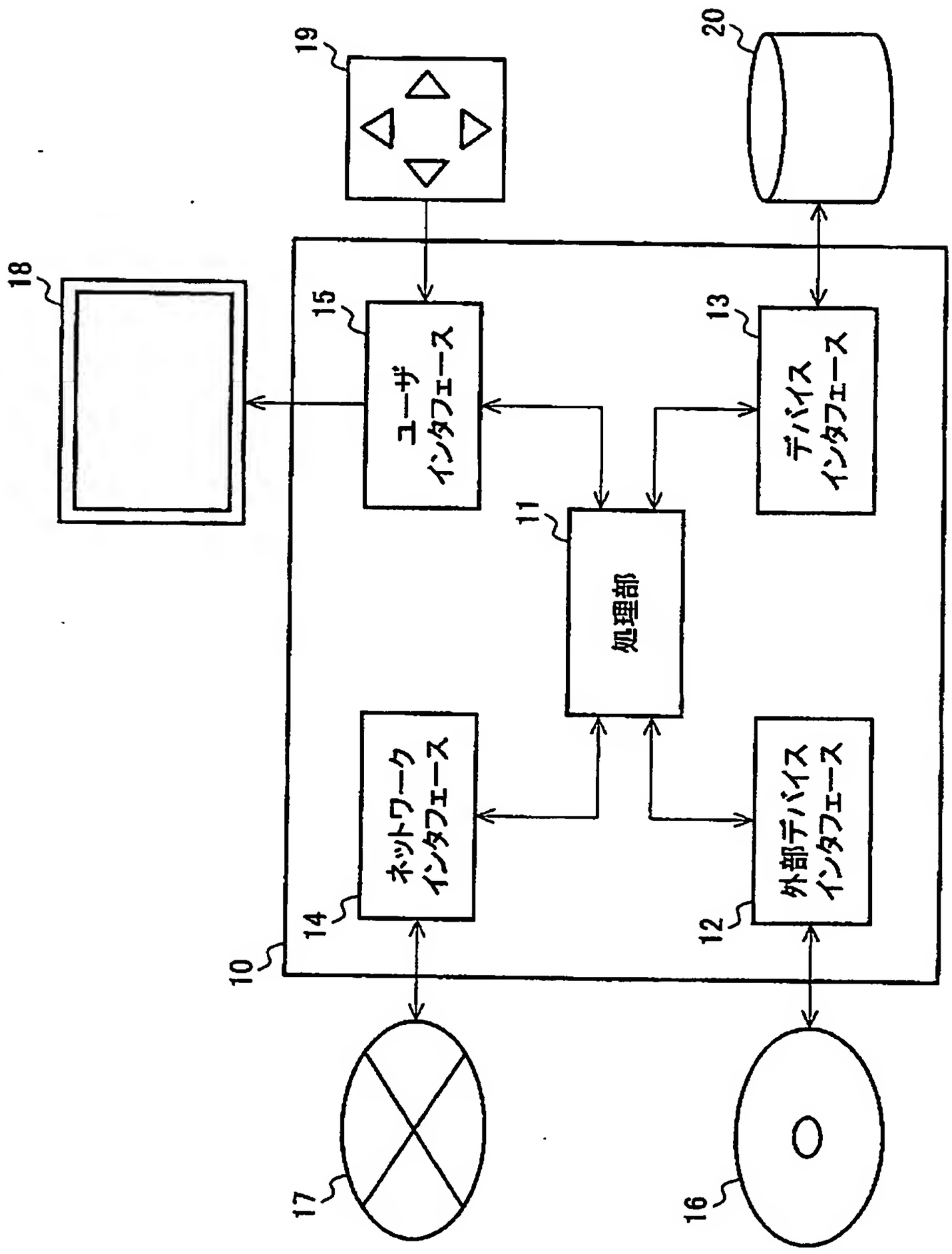
【図７】ハードディスクに記録されているファイル構成の一例を示した図である。
【図８】ＲＯＭディスク及びハードディスクに記録されているファイル構成の他の例を示した図である。
【図９】ハードディスクに記録されているファイル構造の他の例を示した図である。
【図１０】３つの信頼性レベルに対して、３つのアクセス制限レベルを適用する一例を示す図である。

【符号の説明】

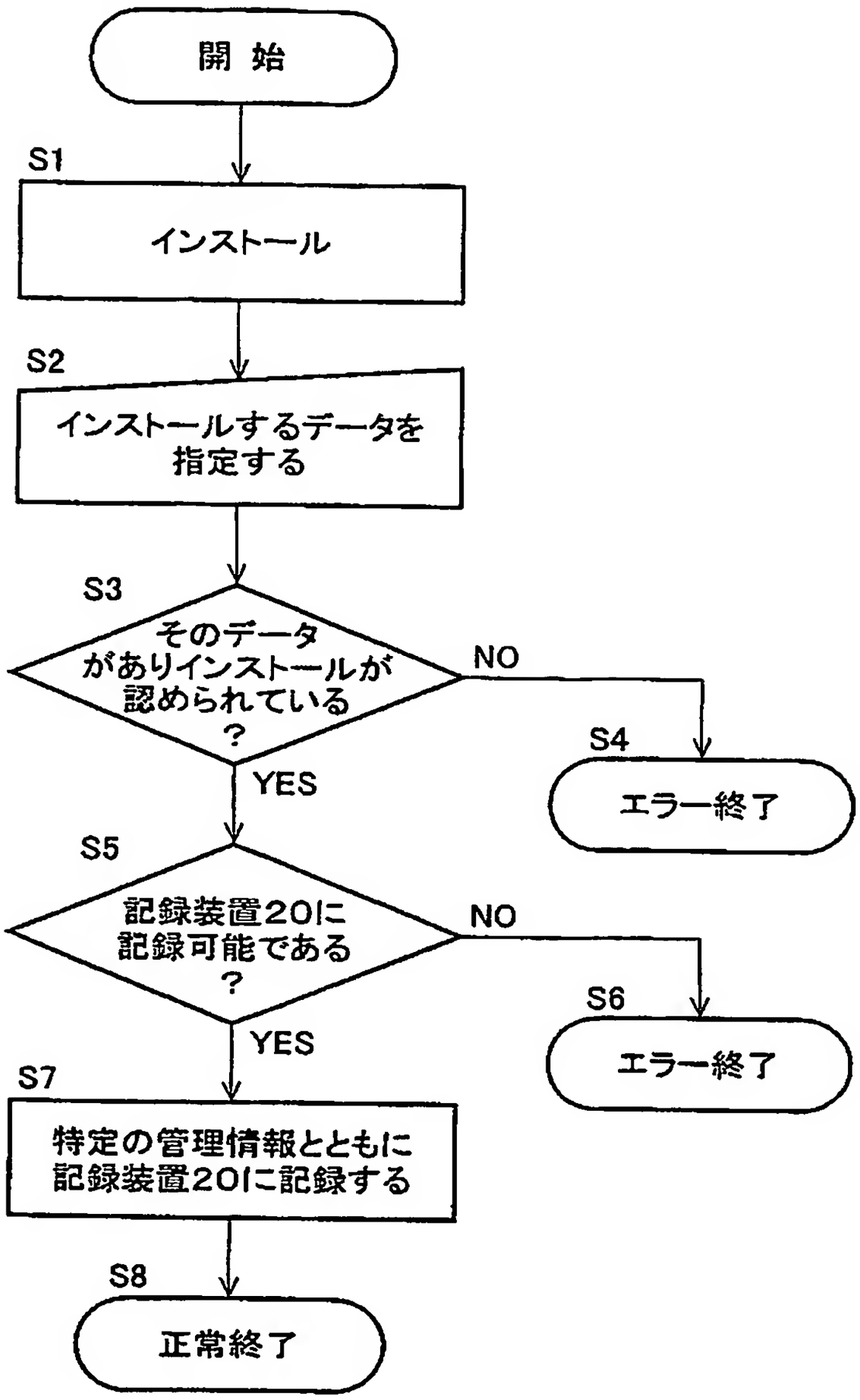
【００９０】

１０…記録再生装置、１１…処理部、１１ａ…アプリケーション実行部、１１ｂ…インストール処理部、１１ｃ…ロード処理部、１１ｄ…メモリ、１２…外部デバイスインタフェース、１３…デバイスインタフェース、１４…ネットワークインタフェース、１５…ユーザインタフェース、１６…外部記録媒体、１７…ネットワーク、１８…ディスプレイ、１９…コントローラ、２０…記録装置（記録媒体）、２０_1，２０_2…記録媒体。

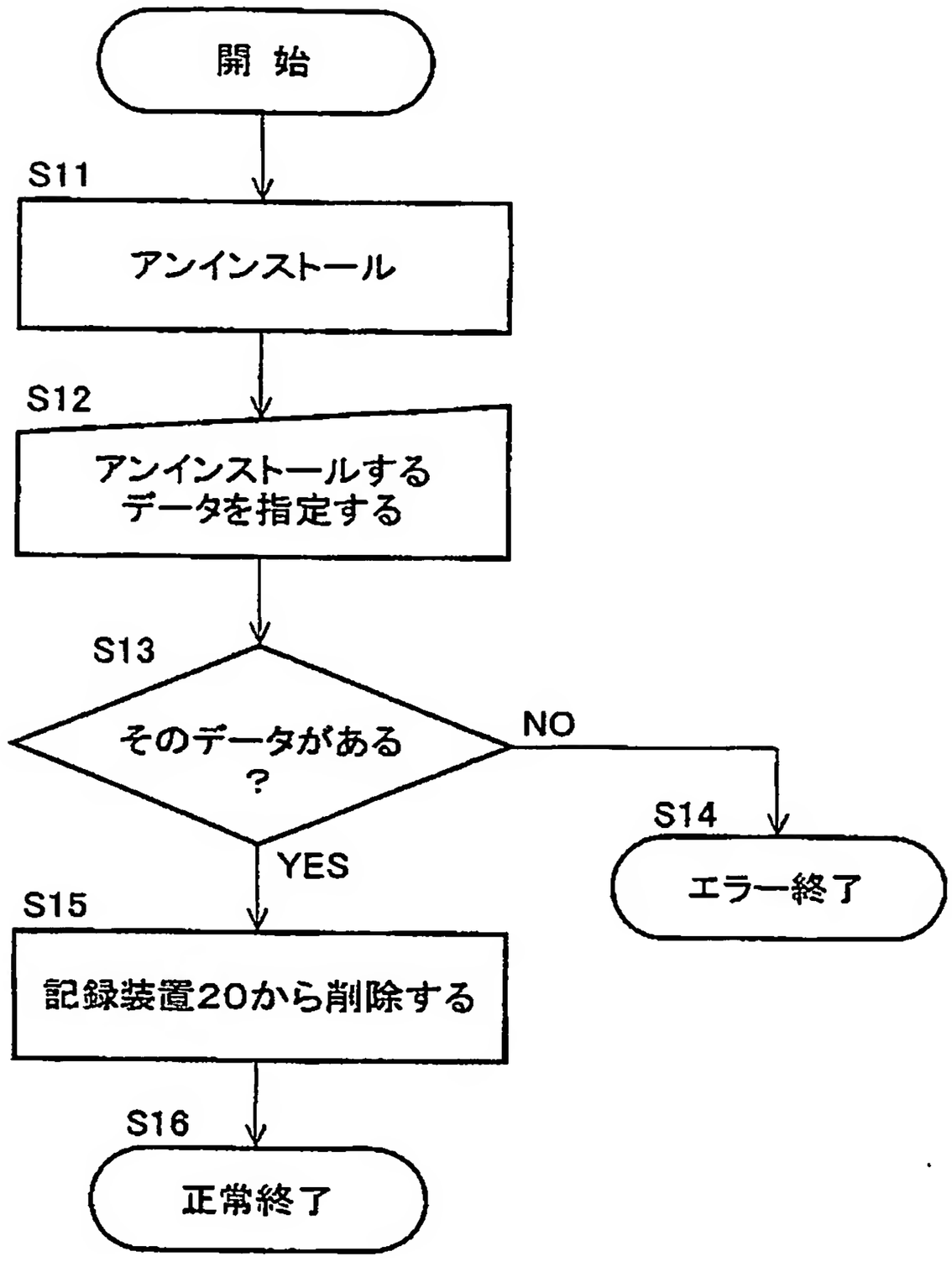
【書類名】図面
【図１】


19
20
18
15
ユーザ
インタフェース
13
デバイス
インタフェース
11
処理部
14
ネットワーク
インタフェース
12
外部デバイス
インタフェース
10
17
16
O

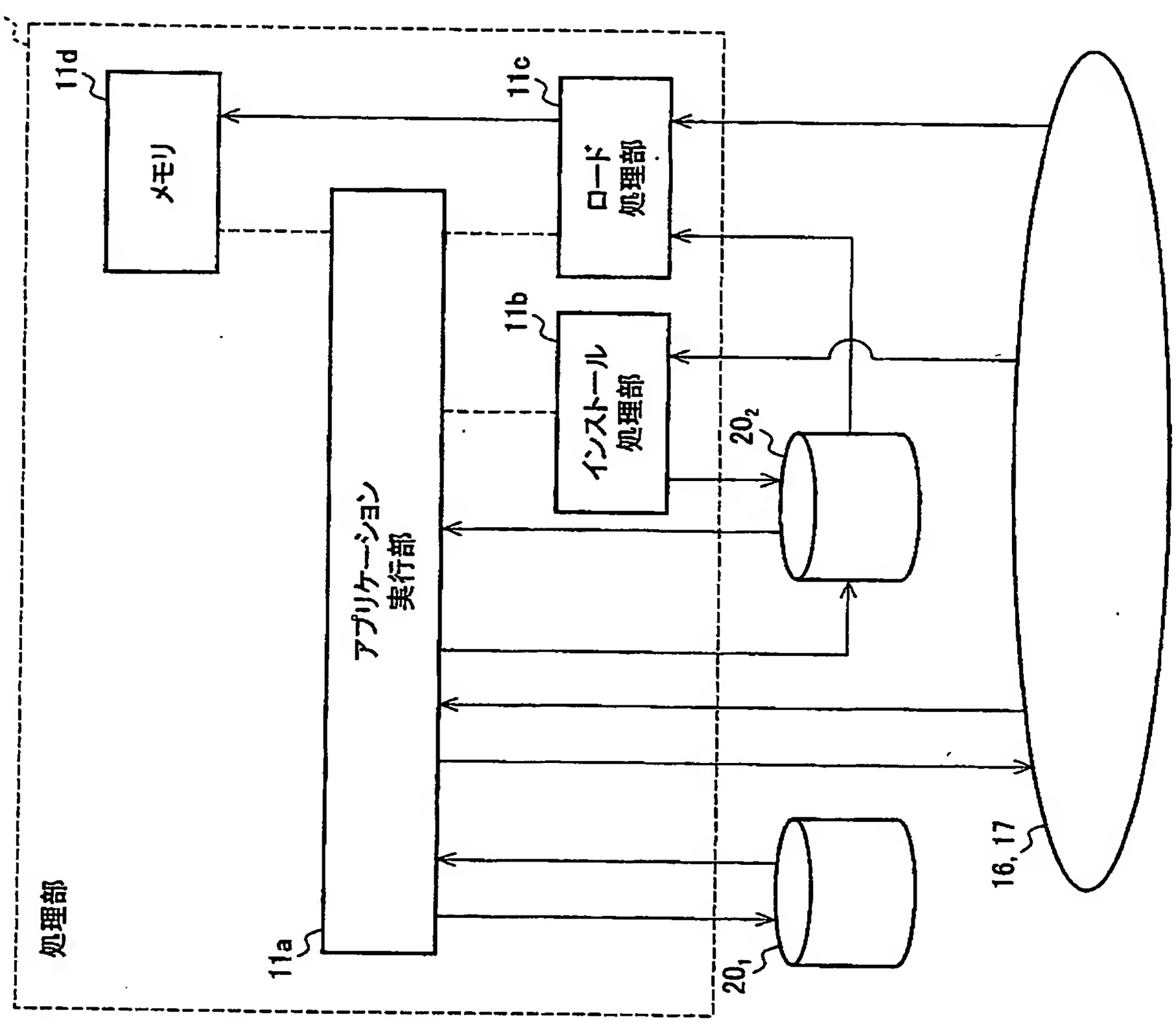
【図２】


開 始
S1
インストール
S2
インストールするデータを
指定する
S3
そのデータ
がありインストールが
認められている
？
NO
S4
エラー終了
YES
S5
記録装置20に
記録可能である
？
NO
S6
エラー終了
YES
S7
特定の管理情報とともに
記録装置20に記録する
S8
正常終了

【図３】


開 始
S11
アンインストール
S12
アンインストールする
データを指定する
S13
そのデータがある
？
NO
S14
エラー終了
YES
S15
記録装置20から削除する
S16
正常終了

【図４】

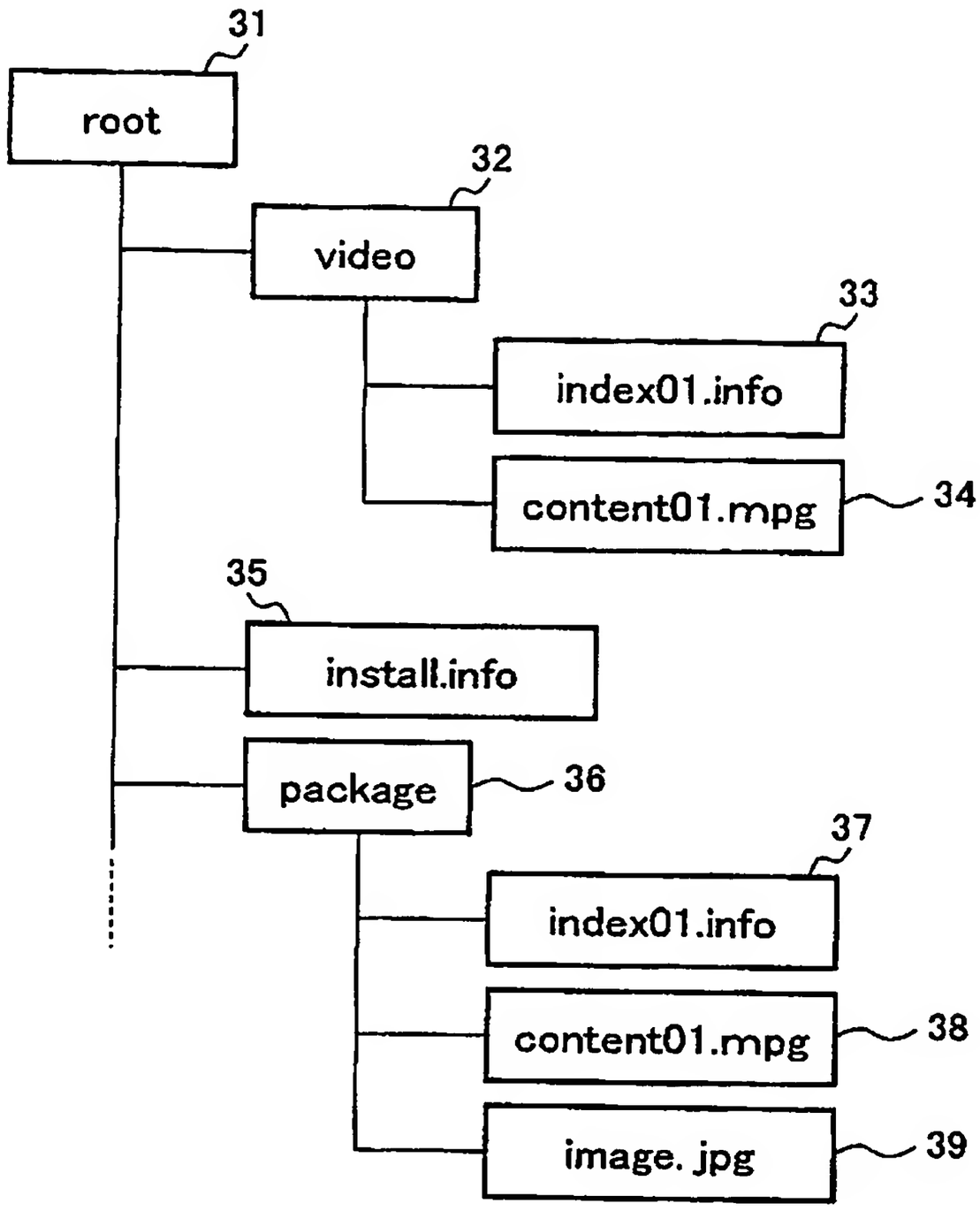

11
処理部
11d
メモリ
11c
ロード処理部
11b
インストール処理部
アプリケーション実行部
11a
20₂
20₁
16,17

【図５】

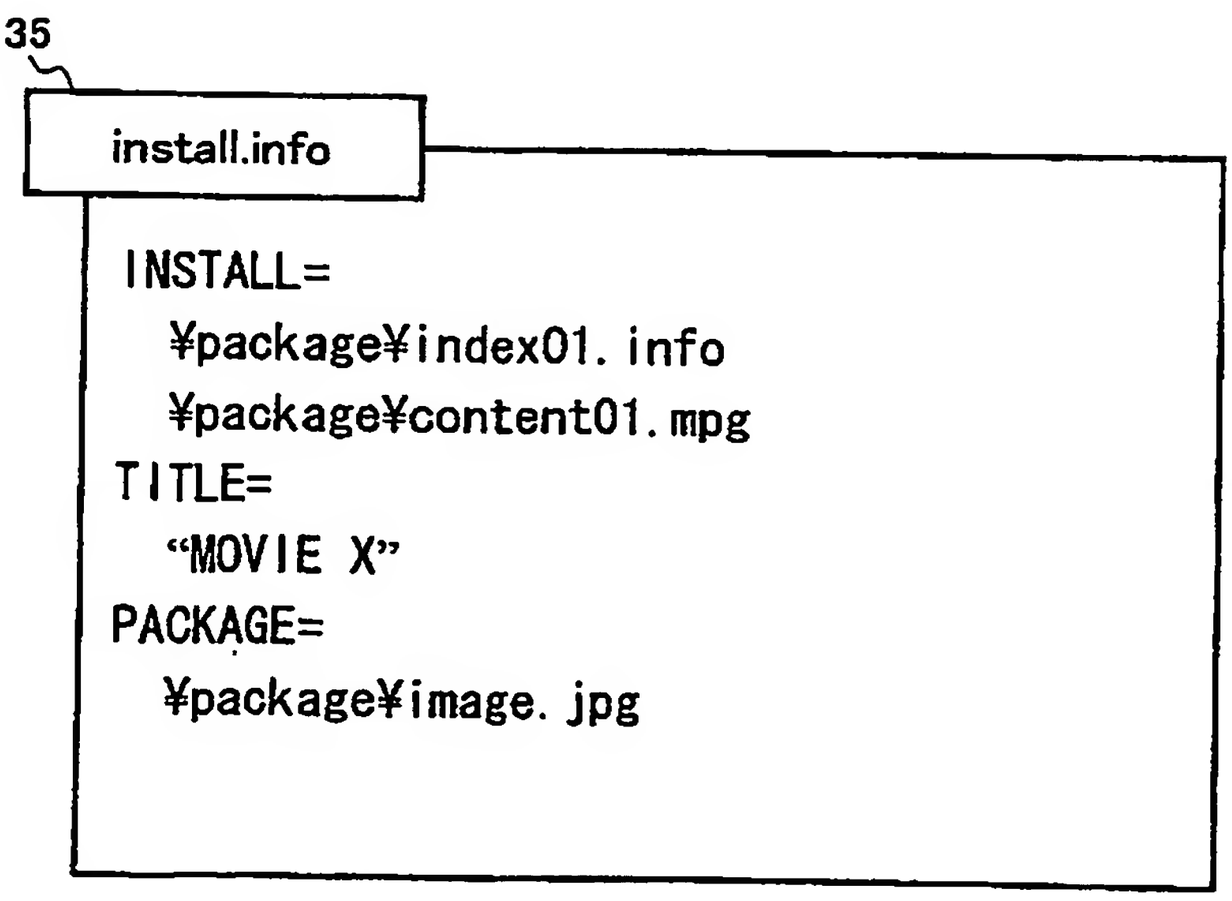
	外部記録媒体16及び記録媒体20_2からの読み込み	外部記録媒体16及び記録媒体20_2への書き出し	記録装置20からの読み込み	記録装置20への書き出し
信頼度大	許可	許可	許可	許可
↑	許可	禁止	許可	許可
信頼度中	許可	禁止	禁止	禁止
↓	禁止	禁止	許可	許可
信頼度小	禁止	禁止	禁止	禁止

【図６】

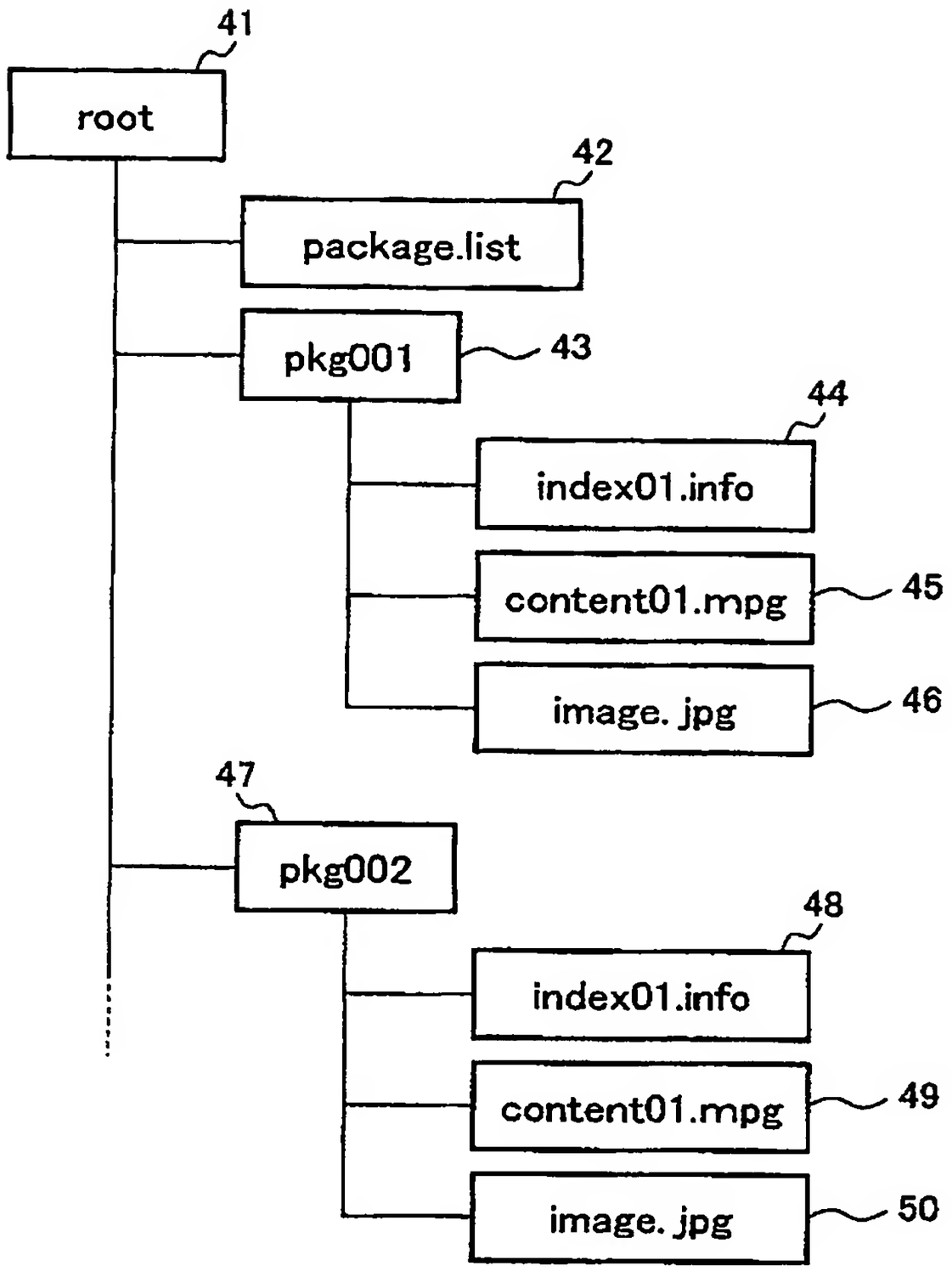
（A）


31
root
32
video
33
index01.info
content01.mpg
34
35
install.info
package
36
37
index01.info
content01.mpg
38
image. jpg
39

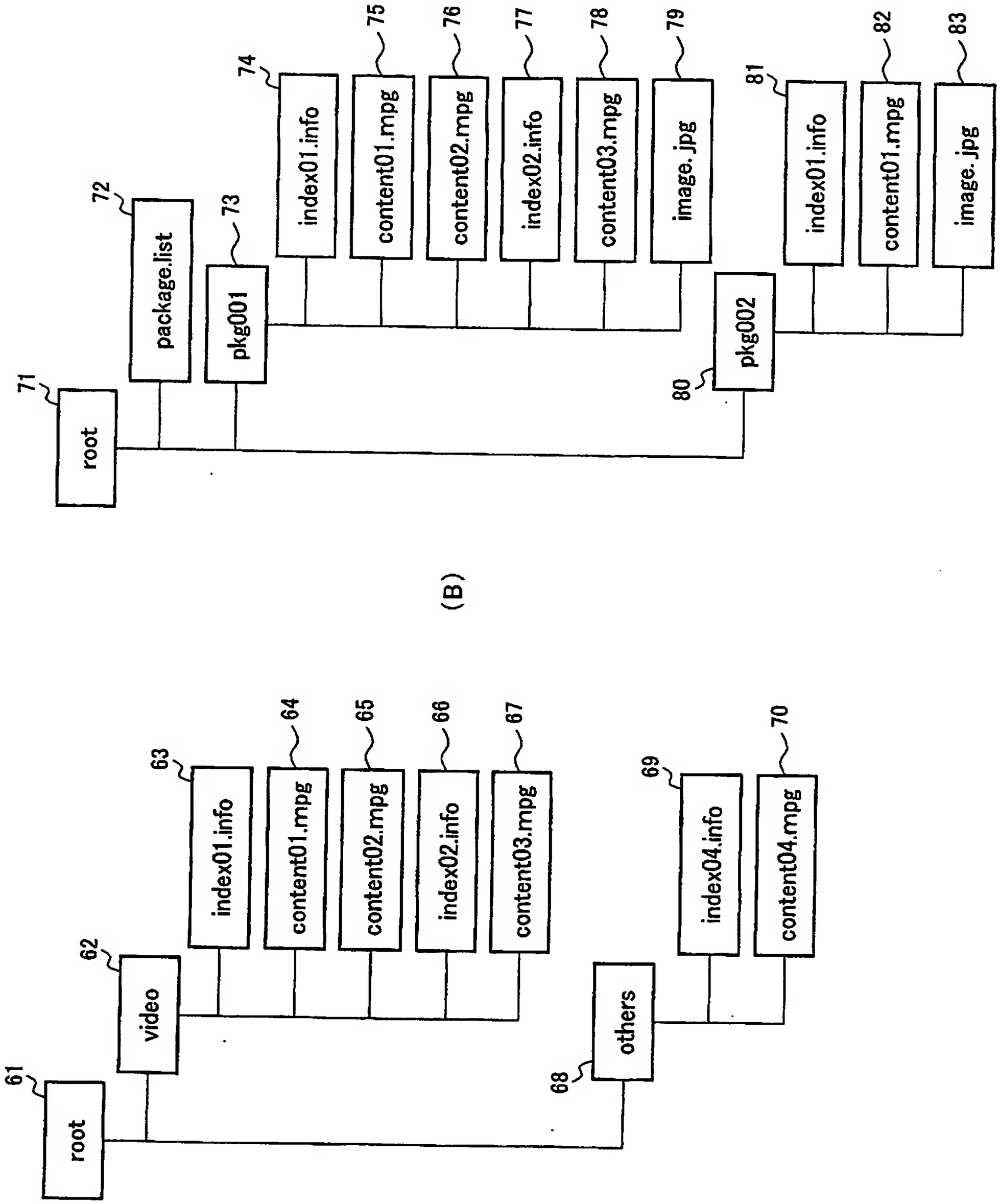
（B）


35
install.info
INSTALL=
¥package¥index01. info
¥package¥content01. mpg
TITLE=
“MOVIE X”
PACKAGE=
¥package¥image. jpg

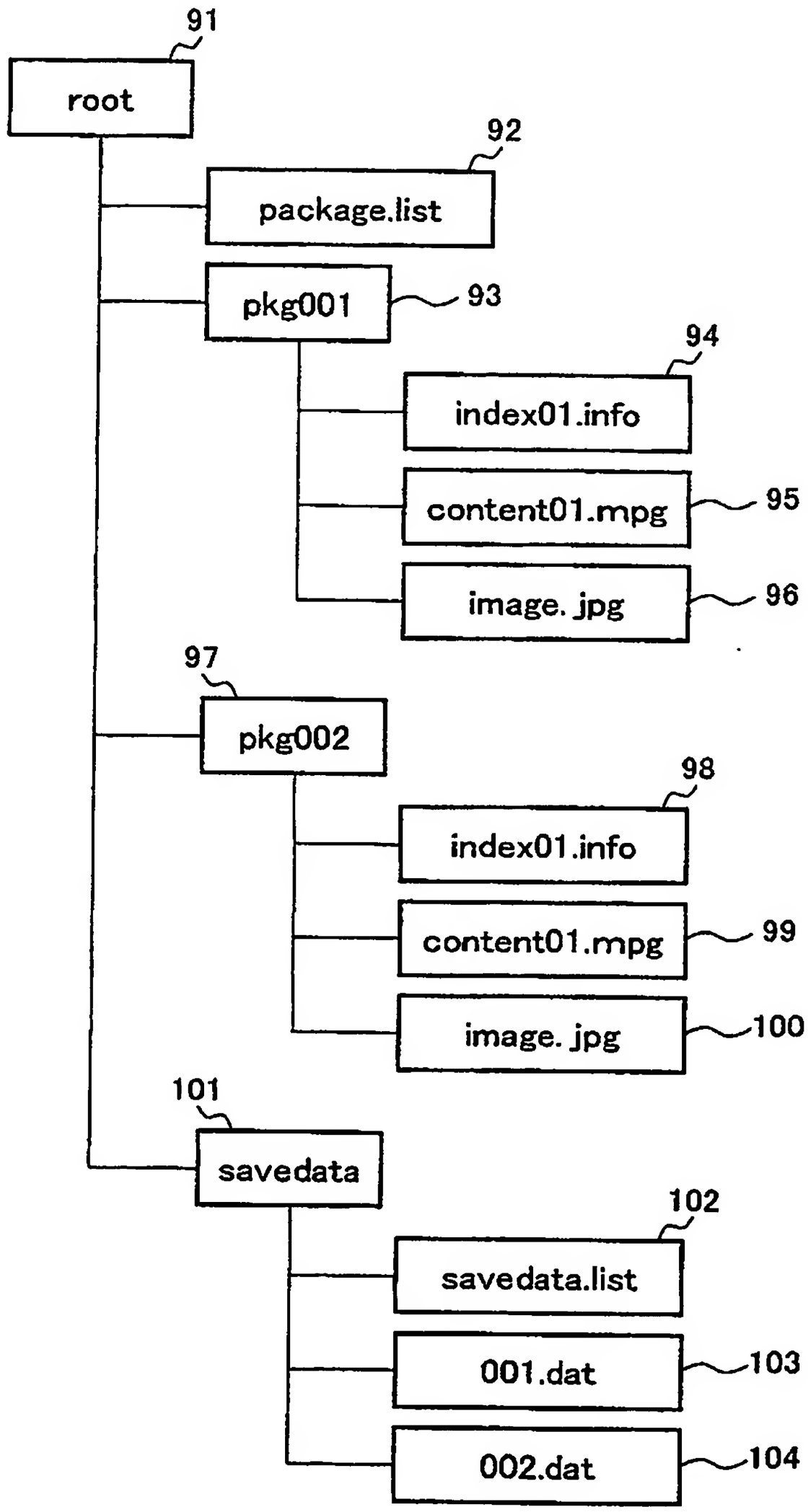
【図７】


41
root
42
package.list
pkg001
43
44
index01.info
content01.mpg
45
image. jpg
46
47
pkg002
48
index01.info
content01.mpg
49
image. jpg
50

【図８】


root
71
package.list
72
pkg001
73
index01.info
74
content01.mpg
75
content02.mpg
76
index02.info
77
content03.mpg
78
image.jpg
79
pkg002
80
index01.info
81
content01.mpg
82
image.jpg
83
(B)
root
61
video
62
index01.info
63
content01.mpg
64
content02.mpg
65
index02.info
66
content03.mpg
67
others
68
index04.info
69
content04.mpg
70
(A)

【図９】


91
root
92
package.list
pkg001
93
94
index01.info
content01.mpg
95
image. jpg
96
97
pkg002
98
index01.info
content01.mpg
99
image. jpg
100
101
savedata
102
savedata.list
001.dat
103
002.dat
104

【図１０】

	ROMディスク16からの読み込み	ハードディスク20のsavedataからの読み込み	ハードディスク20のsavedataへの書き出し	ハードディスク20のパッケージへの書き出し
第1の信頼性レベル（信頼できる）	許可	許可	許可	禁止
第2の信頼性レベル（やや信頼できる）	禁止	許可	許可	禁止
	許可	禁止	禁止	禁止
第3の信頼性レベル（信頼できない）	禁止	禁止	禁止	禁止

【書類名】要約書
【要約】
【課題】外部記録媒体等からコンテンツをインストールして再生又は実行する記録再生装置において、任意のコンテンツに対してアクセス制限を付加することで、該コンテンツによる不正コピーや改ざんを防止する。
【解決手段】記録再生装置１０は、ＡＶデータ又はアプリケーションプログラムを含むコンテンツを記録した外部記録媒体１６を接続する外部デバイスＩ／Ｆ１２と、外部記録媒体１６から読み込んだコンテンツを記録する記録装置２０と、記録したコンテンツを再生又は実行する処理部１１とを有する。処理部１１は、記録再生装置１０によって再生又は実行可能な任意のコンテンツに対して、インストール処理，ロード処理，コンテンツ実行処理に応じて異なるアクセス制限を付加し、コンテンツ実行処理においてはコンテンツのアクセスを該コンテンツの信頼度に応じて制限する。
【選択図】図１

特願２００３－３４６２１７

出　願　人　履　歴　情　報

識別番号　［０００００５０４９］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　シャープ株式会社

出証番号　出証特２００４－３０７９１８８